First Security Islami Bank Limited
ICT Division
Head Office
Plot#12, 2nd & 3rd Floor, Main Road.
Block # A, P.S- Badda,
Bashundhara R/A, Dhaka-1229.
Web: www.fsiblbd.com; email: ict@fsiblbd.com

Ref: FSIBL/HO/ICT/253/2023 Date: 05.03.2023

REQUEST FOR PROPOSAL (RFP)

For Purchasing 2 units DMZ and 2 units Utility Next Generation Firewall at Data Center for 3 (three) years.

Bidder Reg. No.

Section A: General Information

SN	Item		Description				
1	**Name of the Bank**		**First Security Islami Bank Limited**				
2	**Procuring Entity Name**		Information & Communication Technology Division				
3	**Invitation of tender for**		Supply & implementation of **2 units DMZ and 2 units Utility Next Generation Firewall at Data Center** as per technical specifications detailed in "Section C" hereunder from the eligible and registered Partners as specified in "Section B" hereunder.				
4	**Invitation for Quotation Ref. & Date**		FSIBL/HO/ICT/253/2023 Date: 05.03.2023				
5	**Procurement Method**		Open Tendering Method				
6	**Source of Fund**		**First Security Islami Bank Limited**				
7	**Registration of bidders & price of Tender Document:**		The interested eligible bidders have to enroll their name by submitting a prayer along with a non-refundable registration/enrollment fee **Tk. 10,000.00 (Taka Ten Thousand)** only in the form of "Payment Order" in favor of "**First Security Islami Bank Limited** during submission of tender. No Tender documents will be sold physically. The bidder has to copy or download this tender document from the website: www.fsiblbd.com/tender and place them on their own letterhead to submit their bid.				
8	**Tender Process Dates & Times**	**Tender Process**	**Registration**		**Submission**		**Opening Time**
			Start	**End**	**Start**	**End**	
		Date	05.03.2023	28.03.2023	28.03.2023	28.03.2023	28.03.2023
		Time	10.00 AM	02:00 PM	02:00 PM	03:00 PM	03:20 PM
	Pre-bid Schedule	**Date**	12.03.2023				
		Time	11:30 AM				
9	**Place of opening and receiving tender documents**		**First Security Islami Bank Limited**, Plot#12, 3rd Floor, Main Road. Block # A, P.S- Badda, Bashundhara R/A, Dhaka-1229.				
10	**Composition of bid Price shall be inclusive of**		The costs of complete purchasing 2 units DMZ and 2 units Utility Next Generation Firewall as instructed by the bank, testing, commissioning, delivering to directed site and admissible VAT, excise duty, subsidiary duty, import duty, ATV, AIT etc. all types of taxes and revenues of the government and other regulatory authorities along with time value of money up to settlement of bills taking clearances from the end user of the bank.				
11	**Awarding the successful bidder**		The bank may negotiate with the successful bidder or all bidders regarding price reduction modification, if necessary, before issuing the acceptance letter. A notification of award (NOA) will be provided by Bank to the successful bidder. Within 07 days of receipt of the Letter of Acceptance, the successful bidder shall sign a copy of it and return to the bank. Work must be completed within the time specified in the Work Order/Contract.				
12	**Payment & Security**		The bidder shall furnish as bid security of 2.50% of the total financial offer in the form of bank draft or bank guarantee in the form of pay order or bank guarantee from any scheduled bank in favor of First Security Islami Bank Limited. The bid				

SN	Item	Description
		security shall be submitted along with the tender inside the envelop marked as "Financial Offer- for **2 units DMZ and 2 units Utility Next Generation Firewall for FSIBL Data Center**" The bid security should be valid for 60 days after the date of bid opening. Any bid not accompanied by an acceptable bid security shall be rejected as non-responsive. The bid security of unsuccessful bidders will be returned within 7 days from the date awarding the successful bidder. The bid security of the successful bidder will be returned when the bidder has signed the NOA and furnished the required performance security. The bid security may be forfeited if (a) the bidder withdraws its bid during the period of bid validity specified in the bid form; (b) if a successful bidder fails to sign the contract and (c) if a successful bidder fails to furnish the performance security.
		Within 07 days of receipt of the notification of award from the Bank, the successful bidder shall furnish as performance security of 10% of total amount in the form of pay order or bank guarantee from any scheduled bank in favor of First Security Islami Bank Limited. The performance security should be valid for 180 (one hundred eighty) days.
		Bid shall remain valid for a period of 3 (Three) months after the date of opening of the proposals. In exceptional circumstances, prior to expiry of the original bid validity period, the Bank may request the bidder to extend the period of validity for a specified additional period. The request and the responses shall be made in writing. A bidder agreeing to the request will not be permitted to modify its bid.
		50% payment of total price may be provided as an advance payment upon request of the successful bidder. 50% payment may made after implementation of firewall with licenses in its environment for DC upon getting satisfactory certificate from ICT Division, FSIBL, Head Office expressing clearly that the end user has no objection.
		In case of a failure of the successful Bidder to deliver next generation firewall with license in the prescribed time, the bidder will be liable to pay 0.5% of the Contract price as liquidated damages for every week after the deadline and will be deducted from the bill amount. The maximum penalty will be 10% of total contact price.
13	**Submission of bidders Qualifications/Eligibility and curse of bidder**	The interested registered bidder shall copy the "bidders' qualification" form from the webpage and place them on their own letterhead write their qualifications and individual information in a separate sealed envelope with proper labeling mentioning- "Bidder's Qualifications /Eligibility for supplying & implementation of Next Generation Firewall " license, Name of the bidder & Registration No.
14	**Submission of Technical & Financial Offer**	The interested registered bidder shall copy the Asked Technical Specifications and Financial Offer form from the webpage and place them on their own letterhead and write their price offer for Section "C" in the designated field(s) and submit the document in a separate sealed envelope with proper labeling mentioning- "Financial Offer- for 2 units DMZ and 2 units utility Next Generation Firewall for FSIBL Data Center", Name of the bidder & Registration No.
15	**Name and address of the Office for receiving tender(s)**	Vice President & Head of ICT Division. First Security Islami Bank Limited, Plot#12, 3rd Floor, Main Road. Block # A, P.S- Badda, Bashundhara R/A, Dhaka-1229.
16	**Address of Official Inviting Tender**	Do.
17	**Contact Details**	Mobile: 01741018603, 01715995106 email: infosec@fsiblbd.com
18	**Special Instruction**	The Bank Authority reserves the right to - 1. Explain or clarify the terms of this tender notice in its own way, 2. Bring necessary changes in the notice 3. Increase or decrease the tender quantity 4. Reject the lowest 5. Reject any or all bids 6. Select any bidder deems fit and proper by them 7. Bidder have to bid full of the Section "C" The bank authority can perform all the above things without assigning any reason. The bidder/supplier shall have no right to challenge the decision of the Bank Authority in any court of law or to any arbitrator.

REQUEST FOR PROPOSAL (RFP)

For Purchasing 2 units DMZ and 2 units Utility Next Generation Firewall at Data Center for 3 (three) years.

Tender Ref: FSIBL/HO/ICT/253/2023
Date: 05.03.2023
Bidder Reg. No.

Section B: Bidder's Information and Qualifications/Eligibility

SN	Description	Qualification	Response	Remarks
01	**Name of the Bidder**	Required		Attach NID copy
02	**Designation of the Bidder**	Required		
03	**Company Name**	Required		
04	**Company Type** [Proprietorship, Partnership, Private Limited, Public Limited etc.]	Required		
05	**Website address of the company**	Required		
06	**Bidder's Office Phone No.**	Required		Attach bill copy
07	**Bidder's email address**	Required		Send "Test" mail to ict@fsiblbd.com
08	**Bidder's Mobile No.**	Required		
09	**Verified Business Address**	Required		Attach proof
10	**Name of Contact Person**	Required		Attach NID copy
11	**Designation of the contact Person**	Required		
12	**Official email address**	Required		Send "Test" mail to ict@fsiblbd.com
13	**Valid Trade License No.**	Required		Attach proof
14	**Valid VAT Registration No.**	Required		Attach proof
15	**Valid ETIN**	Required		Attach proof
16	**Valid IRC No.**	Required		Attach proof
17	**Authorization of the Principal**	Required		Attach proof
18	**Bank solvency certificate**	Required		Attach proof
19	**Are you adequately solvent to sale on? Credit for a period of 6 months or more?**	Yes/No.		
20	**Experience: The bidder must have 5 (Five) years of experience for supplying similar hardware & license in at least 5 (five) different reputed commercial bank in Bangladesh.**	Required Bank- WO- Date- Quantity-		Attach proof
21	**Are you Banned by any bank authority or? Government agency?**	Yes/No		

Statement of the bidder: All the above information provided here in above are true. We will supply the order from genuine, valid and lawful sources and will pay all admissible VAT, Tax & other duties as per rule of the Government of Bangladesh.

REQUEST FOR PROPOSAL (RFP)

For Purchasing 2 units DMZ and 2 units Utility Next Generation Firewall at Data Center for 3 (three) years.

Tender Ref: FSIBL/HO/ICT/253/2023
Date: 05.03.2023
Bidder Reg. No

Section C: Technical/Financial Specifications of 4 units Next Generation Firewall

LOT-A

Description	Technical Specifications for 2 Unit DMZ Next-Generation Firewall
Type	Next Generation Enterprise Firewall
Model	Should be mentioned by the bidder
Country of Origin	USA/EU
3rd Party Test Certification	Offered product should not have any observed evasions in 2019 SVM NGFW report of NSS and above 95% security effectiveness. Also, should feature in the top quadrant of the Security Value Map (SVM) of NSS Labs report 2019 for Next Generation Firewall (NGFW)
	The proposed vendor must be in the Leader's quadrant of the Enterprise Firewalls Gartner Magic Quadrant for consecutive 8 years
Equipment Test Certification	NEBS Level 3, FCC Class A, CE Class A, VCCI Class A, cTUVus, CB
No of Units	Two (02) Units in HA for DC
Form factor	Modular or Fixed
Architecture	The NGFW architecture should have Control Plane separated from the Data Plane in the Device architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc). Proposed Firewall should not be proprietary ASIC based in nature & should be open architecture based on multi-core CPU's to protect & scale against dynamic latest security threats.
	Proposed NGFW appliance (Each appliance) must have minimum 1 CPU with 8 Physical Cores from day 1. Virtual core count and ASIC architecture will not be considered.
Memory (DRAM)	16 GB Memory from day 1
Features	Provide complete visibility of Network, all applications (including cloud & SaaS), all users and devices (including all locations) and encrypted traffic
	Reduce attack surface area by enabling business apps, block 'bad' apps, Limit application functions, limit high risk websites and content and require MFA (Multifactor authentication);
	Prevents all known threats – Malware, C&C, Malicious & Phishing Websites and Bad Domains;
	Detect and prevent new threats – unknown malware, zero-day exploits and custom attack behavior;
	The solution should support to protect the mobile workforce by extending the Next-Generation Security Platform to all users, regardless of location. It secures traffic by applying the platform's capabilities to: understand application use; associate the traffic with users and devices; and enforce security policies with next-generation technologies. The solution should Inspect and control applications that are encrypted with SSL/TLS/SSH traffic. Stops threats within the encrypted traffic. The solution should be inbuild or through external device.
Storage	Proposed NGFW appliance must have minimum 120 GB SSD Storage
Interfaces Supported	Minimum 8 x 10/100/1000 and 4 x 1/2.5/5 Gb/ (PoE) copper Interfaces from Day 1
	2 X 1G SFP and 8 X 10G SFP+ populated with 4 x 10G optical transceivers SR from same OEM from day one for each NGFW unit.
	10/100/1000 out-of-band management port (1), HSCI 10 gigabit high availability (1), RJ-45 console port (1), USB port (1), Micro USB console port (1) in addition to requested data interfaces from day 1

Signature & Seal of the bidder

Description	Technical Specifications for 2 Unit DMZ Next-Generation Firewall
	Firewall interface configuration should be flexible and allow the firewall to use as perimeter firewall with interface working in layer 3 inspection mode and use other interfaces in IPS mode to monitor traffic of other segments such as MPLS, server zone without requiring any IP configuration on such monitoring interface. Firewall should allow to use all threat inspection and prevention policies on perimeter layer and monitoring interface zones at the same time. This functionality should not require virtualization to be enabled on firewall and run both mentioned modes concurrently without compromising any performance or features
Performance Capacity	Next Gen Firewall application throughput – Minimum 9.5 Gbps
	Next Gen Threat prevention throughput – minimum 5 Gbps
	Minimum IPsec VPN throughput – 6.5 Gbps
	Minimum client agent tunnels (SSL, IPSec, and IKE (V1 & V2 supported with XAUTH)
	Proposed appliance should support Minimum New sessions per second –120K utilizing 1 byte HTTP transactions
	Proposed appliance should support Minimum Concurrent Connection per second with threat prevention features enabled – 1.4 million
High Availability	Active/Active and Active/Passive
Application Control Throughput	A Minimum NG Firewall application throughput in real world/production environment measured with Application Control and logging enabled using 64 KB HTTP transactions size /appmix transactions – 9.5 Gbps. Asked performance throughput must be deliver by each appliance, it should not be consolidated throughput of multiple appliance cluster or context. The bidder shall submit the performance test report from Global Product Engineering department / Global Testing Department/ Global POC team of OEM to certify the mentioned performance.
Total Threat Protection Throughput	Minimum NG Threat prevention throughput in real world/production environment measured with Application control, IPS, antivirus, anti-spyware, Zero-day protection, file blocking, and logging enabled, utilizing 64 KB HTTP transactions size /appmix transactions –5 Gbps. Asked performance throughput must be deliver by each appliance, it should not be consolidated throughput of multiple appliance cluster or context. The bidder shall submit the performance test report from Global Product Engineering department / Global Testing Department/ Global POC team of OEM to certify the mentioned performance.
Interface Operation Mode	The proposed firewall shall support Dual Stack IPv4 / IPv6 application control and threat inspection support in: - Tap Mode - Transparent mode (IPS Mode) - Layer 2 - Layer 3 - Should be able operate mix of multiple modes
SD-WAN	Proposed NGFW should have SD-WAN ready and can be activated by procuring licensing as and when require.
	Should support Link metric collection, jitter, drop, delay
	Application and network condition aware sub-second steering
	Session-based link aggregation
	Should support Intelligent path selection based on metric; dynamic application steering
	Scalable bidirectional path health measurements, QoS, traffic shaping
	Predefined application thresholds for common application categories
Next Generation Firewall Features	The proposed firewall shall have network traffic classification which identifies applications across all ports irrespective of port/protocol/evasive tactic.
	The proposed firewall shall be able to handle (alert, block or allow) unknown / unidentified applications like unknown UDP & TCP
	The OEM must provide free professional security audit reports once every 3 months after studying the Bank network. The report must provide details related to discovery of all types of threats (known and unknown) that are running on the network. It should also cover bandwidth utilization of all applications by user, and capture the threat landscape suggesting corrective action if required. The Bidder is duty bound to include implementation as part of this exercise. Please note that all such security reports will be the property of the Bank.
	The proposed firewall shall be able to create custom application signatures and categories using the inline packet capture feature of the firewall without any third-party tool or technical support.
	The proposed firewall shall be able to implement Zones, IP address, Port numbers, User id, Application id and threat protection profile under the same firewall rule or the policy configuration
	The proposed firewall shall delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability inside the chat application base on the content.

Signature & Seal of the bidder

Description	Technical Specifications for 2 Unit DMZ Next-Generation Firewall
	The proposed firewall shall be able to protect the user from the malicious content upload or download by application such as Facebook chat or file sharing by enforcing the total threat protection for known and unknown malicious content such as virus, malware or a bad URLs.
	The proposed firewall shall be able to identify, decrypt and evaluate SSL traffic in an outbound connection (forward-proxy) and inbound connection. The proposed firewall shall be able to identify, decrypt and evaluate SSH Tunnel traffic in an inbound and outbound connections
	The proposed firewall shall be able to identifies port-based rules/policies so admin / security team can convert them to application-based whitelist rules or add applications to existing rules without compromising application availability.
	The proposed firewall shall be able to identifies the rules configured with unused applications and prioritize which rules to migrate or clean up first
	The proposed firewall shall be able restrict application traffic to its default ports to prevent evasive applications from running on non-standard ports.
	The proposed firewall should have data filtering features to prevent sensitive, confidential, and proprietary information from leaving network
	The Firewall should allow conversion of legacy firewall rules into app-based rules. The vendor should provide seamless adoption of application-based rules without compromising application availability. It should automatically identify rules configured with unused applications and suggest the right applications that should be enforced.
	The Firewall should always be accessible irrespective of the load of traffic on the firewall. There should not be an instance when firewall becomes inaccessible during heavy traffic situations. There should be dedicated resources allocated within the firewall for firewall management, logging, reporting etc.
	The solution should have capabilities to evaluate proposed firewall configuration by measuring the adoption of capabilities, validating whether the policies adhere to best practices, and providing recommendations and instructions for how to remediate failed best practice checks.
	The Firewall should provide detailed Change monitor or baseline deviations applications, source and destinations. The change monitor dashboard should compare changes in applications, source and destinations in terms of percentage increase/decrease for last 15 mins/ 30 mins/ one hour/ one day against historical time period of 24 hours/ 7 days/ one month etc.
Threat Protection	Should support protocol decoder-based analysis stateful decodes the protocol and then intelligently applies signatures to detect network and application exploits
	Intrusion prevention signatures should be built based on the vulnerability itself, A single signature should stop multiple exploit attempts on a known system or application vulnerability.
	Should block known network and application-layer vulnerability exploits
	The proposed firewall shall perform content-based signature matching beyond the traditional hash base signatures
	The proposed firewall shall have on box Anti-Virus/Malware, Anti Spyware signatures and should have minimum signatures update window of every one hour
	All the protection signatures should be created by vendor based on their threat intelligence and should not use any 3rd party IPS or AV engines.
	Should perform stream-based Anti-Virus inspection and not store-and-forward traffic inspection to keep the maximum firewall performance. Stream based Antivirus scanning should be used for scanning the contents of the files being transferred over the wire for virus/malwares and should block the file transfer when a virus or malware signatures is triggered.
	Should be able to perform Anti-virus scans for SMB traffic
	Should support DNS sink holing for malicious DNS request from inside hosts to outside bad domains and should be able to integrate and query third party external threat intelligence databases to block or sinkhole bad IP address, Domain and URLs
	Should be able to call 3rd party threat intelligence data on malicious IPs, URLs and Domains to the same firewall policy to block those malicious attributes and list should get updated dynamically with latest data
	Vendor should automatically push dynamic block list with latest threat intelligence database on malicious IPs, URLs and Domains to the firewall policy as an additional protection service
	Solution must prevent sensitive information such as credit card or social security numbers from leaving a protected network from day one. It should also allow administrator to filter on key words, such as a sensitive project name or the word confidential.
	Solution must prevent sensitive information such as credit card or social security numbers from leaving a protected network from day one. It should also allow administrator to filter on key words, such as a sensitive project name or the word confidential.

Signature & Seal of the bidder

Description	Technical Specifications for 2 Unit DMZ Next-Generation Firewall
	The NGFW should prevent credential theft attack. Vendor should provide features with the ability to prevent the theft and abuse of stolen credentials, one of the most common methods of cyber adversaries use to successfully compromise and maneuver within an organization to steal valuable assets. It should also complement additional malware and threat prevention and secure application enablement functionality, to extend customer organizations' ability to prevent cyber breaches. · Automatically identify and block phishing sites · Prevent users from submitting credentials to phishing sites · Prevent the use of stolen credential
Advanced Persistent Threat (APT) Protection	This should have Inline prevention capabilities to stop patient zero threats without affecting productivity.
	The proposed solution should have signatureless approach to prevent unknown weaponized files, credential phishing, and malicious scripts instantly / real time without holding files or web pages without configuring MTA or sending to cloud for analysis.
	The proposed solution should identify variants of known malware in real-time without sending to cloud for analysis.
	This should be a cloud base unknown malware analysis service with guaranteed protection signature delivery time not more than ten seconds
	Advance unknown malware analysis engine should be capable of machine learning with static analysis and dynamic analysis engine with custom-built virtual hypervisor analysis environment
	Advance unknown malware analysis engine with real hardware, detecting VM-aware malware to detect and protect from on-premise /virtual sandbox evading advance unknown malware
	Cloud base unknown malware analysis service should be certified with SOC2 or any other Data privacy compliance certification for customer data privacy protection which is uploaded to unknown threat emulation and analysis
	Cloud base unknown malware analysis service should be able to perform dynamic threat analysis on such as EXEs, DLLs, ZIP files, PDF documents, Office Documents, Java®, Android APKs, Adobe Flash applets, Web pages that include high-risk embedded content like JavaScript, Adobe Flash files. MAC OS and DMG file types
	The proposed next generation security platform should be able to detect and prevent zero-day threats infection through HTTP, HTTPS, FTP, SMTP, POP3, IMAP use by any of application used by the users (e.g: Gmail, Facebook, MS outlook)
	Advance unknown malware analysis engine with real hardware, detecting VM-aware malware to detect and protect from virtual sandbox evading advance unknown malware
	Solution should detonate evasive threats in a real hardware environment, entirely removing an adversary's ability to deploy anti-VM analysis techniques
	Advance unknown malware analysis engine should be able to creates automated high-fidelity signature for command and control connections and spyware to inspect command and control http payload to create one to many payload base signatures protection from multiple unknown spyware and command and control channels using single content base signature
	The protection signatures created base unknown malware emulation should be payload or content base signatures that could block multiple unknown malware that use different hash but the same malicious payload.
URL Filtering and Web Protection	Same Hardware platform should be scalable to provide URL filtering and web protection and should maintain same performance/throughputs mention in primary scope
	The proposed firewall shall have the database located locally on the device
	The proposed firewall shall have custom URL-categorization
	The proposed firewall shall have customizable block pages capability
	The proposed firewall shall block and continue (i.e. allowing a user to access a web-site which potentially violates policy by presenting them a block page with a warning with a continue option allowing them to proceed for a certain time)
	The proposed firewall shall have logs populated with end user activity reports for site monitoring within the local firewall
	The proposed firewall shall have Drive-by-download control
	The proposed firewall shall have URL Filtering policies by AD user, group, machines and IP address/range
	Should have full-path categorization of URLs only to block re categories the malicious malware path not the full domain or website
	Should have zero-day malicious web site or URL blocking update less than 15 minutes for URL DB update for zero-day malware command and control, spyware and phishing websites access protection

Signature & Seal of the bidder

Description	Technical Specifications for 2 Unit DMZ Next-Generation Firewall
	Should have URL or URL category base protection for user cooperate credential submission protection from phishing attack with malicious URL path
SSL/SSH Decryption	The proposed firewall shall be able to identify, decrypt and evaluate SSL traffic in an outbound connection (forward-proxy)
	The proposed firewall shall be able to identify, decrypt and evaluate SSL traffic in an inbound connection
	The proposed firewall shall be able to identify, decrypt and evaluate SSH Tunnel traffic in an inbound and outbound connections
	The NGFW shall support the ability to have a SSL inspection policy differentiate between personal SSL connections i.e. banking, shopping, health and non-personal traffic
	SSL decryption must be supported on any port used for SSL i.e. SSL decryption must be supported on non-standard SSL port as well
	The NGFW shall support TLS version 1.3
Network Address Translation	The proposed firewall must be able to operate in routing/NAT mode
	The proposed firewall must be able to support Network Address Translation (NAT)
	The proposed firewall must be able to support Port Address Translation (PAT)
	The proposed firewall shall support Dual Stack IPv4 / IPv6 (NAT64, NPTv6)
	Should support Dynamic IP reservation, tunable dynamic IP and port over subscription
IPv6 Support	L2, L3, Tap and Transparent mode
	Should support on firewall policy with User and Applications
	Should support SSL decryption on IPv6
	Should support SLAAC Stateless Address Auto configuration
Routing and Multicast support	The proposed firewall must support the following routing protocols: - Static - RIP V1/V2 - OSPFv2/v3 with graceful restart - BGP v4 with graceful restart
	Policy-based forwarding
	PIM-SM, PIM-SSM, IGMP v1, v2, and v3
	Bidirectional Forwarding Detection (BFD)
Authentication	should support the following authentication protocols: - LDAP - Radius (vendor specific attributes) - Token-based solutions (i.e. Secure-ID) - Kerberos
	The proposed firewall's SSL VPN shall support the following authentication protocols - LDAP - Radius - Token-based solutions (i.e. Secure-ID) - Kerberos - SAML - Any combination of the above
Monitoring, Management and Reporting	Should support on device management with complete feature parity on firewall administration
	Should have real time logging based on all Traffic, Threats, User IDs, URL filtering, Data filtering, Content filtering, unknown malware analysis, Authentication, Tunneled Traffic and correlated log view base on other logging activities
	Should support the report generation on a manual or schedule (Daily, Weekly, Monthly, etc.) basis
	Should allow the report to be exported into other format such as PDF, HTML, CSV, XML etc.
	Should have built in report templates based on Applications, Users, Threats, Traffic and URLs
	Should be able to create report based on SaaS application usage
	Should be able to create reports based on user activity
	Should be able to create custom report based on custom query base any logging attributes
	On-device management service should be able to provide all the mentioned features in case of central management server failure
Authorization	Original Manufacturer Authorization Certificate to be submitted along with the bid

Signature & Seal of the bidder

Description	Technical Specifications for 2 Unit DMZ Next-Generation Firewall
	3 Years OEM Premium support bundle including parts & labor with 24x7x365 days TAC support, RMA, software updates and subscription update support. The NGFW should be proposed with 3 years subscription licenses for (i) Zero-Day Threat Protection (ii) NGFW (iii) NGIPS (iv) Anti-Virus (v) Anti Spyware, (vi) Anti Botnet (vii) Anti APT and (viii) URL-Filtering
Cross Reference	Bidders has to provide public reference documents/links for each specification points mentioned in the above for verification.

LOT-B

Description	Technical Specifications 2 Unit Utility Next-Generation Firewall
Type	Next Generation Enterprise Firewall
Model	Should be mentioned by the bidder
Country of Origin	USA/EU
3rd Party Test Certification	Offered product should not have any observed evasions in 2019 SVM NGFW report of NSS and above 95% security effectiveness. Also, should feature in the top quadrant of the Security Value Map (SVM) of NSS Labs report 2019 for Next Generation Firewall (NGFW)
	The proposed vendor must be in the Leader's quadrant of the Enterprise Firewalls Gartner Magic Quadrant for consecutive 8 years
Equipment Test Certification	NEBS Level 3, FCC Class A, CE Class A, VCCI Class A, cTUVus, CB
No of Units	Two (02) Units in HA for DC
Form factor	Modular or Fixed
Architecture	The NGFW architecture should have Control Plane separated from the Data Plane in the Device architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc). Proposed Firewall should not be proprietary ASIC based in nature & should be open architecture based on multi-core CPU's to protect & scale against dynamic latest security threats.
	Proposed NGFW appliance (Each appliance) must have minimum 1 CPU with 8 Physical Cores from day 1. Virtual core count and ASIC architecture will not be considered.
Memory (DRAM)	16 GB Memory from day 1
Features	Provide complete visibility of Network, all applications (including cloud & SaaS), all users and devices (including all locations) and encrypted traffic
	Reduce attack surface area by enabling business apps, block 'bad' apps, Limit application functions, limit high risk websites and content and require MFA(Multifactor authentication);
	Prevents all known threats – Malware, C&C, Malicious & Phishing Websites and Bad Domains;
	Detect and prevent new threats – unknown malware, zero-day exploits and custom attack behavior;
	The solution should support to protect the mobile workforce by extending the Next-Generation Security Platform to all users, regardless of location. It secures traffic by applying the platform's capabilities to: understand application use; associate the traffic with users and devices; and enforce security policies with next-generation technologies. The solution should Inspect and control applications that are encrypted with SSL/TLS/SSH traffic. Stops threats within the encrypted traffic. The solution should be inbuild or through external device.
Storage	Proposed NGFW appliance must have minimum 120 GB SSD Storage
Interfaces Supported	Minimum 8 x 10/100/1000 and 4 x 1/2.5/5 Gb/ (PoE) copper Interfaces from Day 1
	2 X 1G SFP and 8 X 10G SFP+ populated with 4 x 10G optical transceivers SR from same OEM from day one for each NGFW unit.
	10/100/1000 out-of-band management port (1), HSCI 10 gigabit high availability (1), RJ-45 console port (1), USB port (1), Micro USB console port (1) in addition to requested data interfaces from day 1
	Firewall interface configuration should be flexible and allow the firewall to use as perimeter firewall with interface working in layer 3 inspection mode and use other interfaces in IPS mode to monitor traffic of other segments such as MPLS, server zone without requiring any IP configuration on such monitoring interface. Firewall should allow to use all threat inspection and prevention policies on perimeter layer and monitoring interface zones at the same time. This functionality should not require virtualization to be enabled on firewall and run both mentioned modes concurrently without compromising any performance or features
Performance Capacity	Next Gen Firewall application throughput – Minimum 9.5 Gbps
	Next Gen Threat prevention throughput – minimum 5 Gbps

Signature & Seal of the bidder

Description	Technical Specifications 2 Unit Utility Next-Generation Firewall
	Minimum IPsec VPN throughput – 6.5 Gbps
	Minimum client agent tunnels (SSL, IPSec, and IKE (V1 & V2 supported with XAUTH)
	Proposed appliance should support Minimum New sessions per second –120K utilizing 1 byte HTTP transactions
	Proposed appliance should support Minimum Concurrent Connection per second with threat prevention features enabled – 1.4 Million
High Availability	Active/Active and Active/Passive
Application Control Throughput	A Minimum NG Firewall application throughput in real world/production environment measured with Application Control and logging enabled using 64 KB HTTP transactions size / appmix transactions – 9.5 Gbps. Asked performance throughput must be deliver by each appliance, it should not be consolidated throughput of multiple appliance cluster or context. The bidder shall submit the performance test report from Global Product Engineering department / Global Testing Department/ Global POC team of OEM to certify the mentioned performance.
Total Threat Protection Throughput	Minimum NG Threat prevention throughput in real world/production environment measured with Application control, IPS, antivirus, anti-spyware, Zero-day protection, file blocking, and logging enabled, utilizing 64 KB HTTP transactions size / appmix transactions –5 Gbps. Asked performance throughput must be deliver by each appliance, it should not be consolidated throughput of multiple appliance cluster or context. The bidder shall submit the performance test report from Global Product Engineering department / Global Testing Department/ Global POC team of OEM to certify the mentioned performance.
Interface Operation Mode	The proposed firewall shall support Dual Stack IPv4 / IPv6 application control and threat inspection support in: - Tap Mode - Transparent mode (IPS Mode) - Layer 2 - Layer 3 - Should be able operate mix of multiple modes
SD-WAN	Proposed NGFW should have SD-WAN ready and can be activated by procuring licensing as and when require.
	Should support Link metric collection, jitter, drop, delay
	Application and network condition aware sub-second steering
	Session-based link aggregation
	Should support Intelligent path selection based on metric; dynamic application steering
	Scalable bidirectional path health measurements, QoS, traffic shaping
	Predefined application thresholds for common application categories
Next Generation Firewall Features	The proposed firewall shall have network traffic classification which identifies applications across all ports irrespective of port/protocol/evasive tactic.
	The proposed firewall shall be able to handle (alert, block or allow) unknown / unidentified applications like unknown UDP & TCP
	The OEM must provide free professional security audit reports once every 3 months after studying the Bank network. The report must provide details related to discovery of all types of threats (known and unknown) that are running on the network. It should also cover bandwidth utilization of all applications by user, and capture the threat landscape suggesting corrective action if required. The Bidder is duty bound to include implementation as part of this exercise. Please note that all such security reports will be the property of the Bank.
	The proposed firewall shall be able to create custom application signatures and categories using the inline packet capture feature of the firewall without any third-party tool or technical support.
	The proposed firewall shall be able to implement Zones, IP address, Port numbers, User id, Application id and threat protection profile under the same firewall rule or the policy configuration
	The proposed firewall shall delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability inside the chat application base on the content.
	The proposed firewall shall be able to protect the user from the malicious content upload or download by application such as Facebook chat or file sharing by enforcing the total threat protection for known and unknown malicious content such as virus, malware or a bad URLs.
	The proposed firewall shall be able to identify, decrypt and evaluate SSL traffic in an outbound connection (forward-proxy) and inbound connection. The proposed firewall shall be able to identify, decrypt and evaluate SSH Tunnel traffic in an inbound and outbound connections
	The proposed firewall shall be able to identifies port-based rules/policies so admin / security team can convert them to application-based whitelist rules or add applications to existing rules without compromising application availability.
	The proposed firewall shall be able to identifies the rules configured with unused applications and prioritize which rules to migrate or clean up first
	The proposed firewall shall be able restrict application traffic to its default ports to prevent evasive applications from running on non-standard ports.
	The proposed firewall should have data filtering features to prevent sensitive, confidential, and

Signature & Seal of the bidder

Description	Technical Specifications 2 Unit Utility Next-Generation Firewall
	proprietary information from leaving network
	The Firewall should allow conversion of legacy firewall rules into app-based rules. The vendor should provide seamless adoption of application-based rules without compromising application availability. It should automatically identify rules configured with unused applications and suggest the right applications that should be enforced.
	The Firewall should always be accessible irrespective of the load of traffic on the firewall. There should not be an instance when firewall becomes inaccessible during heavy traffic situations. There should be dedicated resources allocated within the firewall for firewall management, logging, reporting etc.
	The solution should have capabilities to evaluate proposed firewall configuration by measuring the adoption of capabilities, validating whether the policies adhere to best practices, and providing recommendations and instructions for how to remediate failed best practice checks.
	The Firewall should provide detailed Change monitor or baseline deviations applications, source and destinations. The change monitor dashboard should compare changes in applications, source and destinations in terms of percentage increase/decrease for last 15 mins/ 30 mins/ one hour/ one day against historical time period of 24 hours/ 7 days/ one month etc.
Threat Protection	Should support protocol decoder-based analysis stateful decodes the protocol and then intelligently applies signatures to detect network and application exploits
	Intrusion prevention signatures should be built based on the vulnerability itself, A single signature should stop multiple exploit attempts on a known system or application vulnerability.
	Should block known network and application-layer vulnerability exploits
	The proposed firewall shall perform content-based signature matching beyond the traditional hash base signatures
	The proposed firewall shall have on box Anti-Virus/Malware, Anti Spyware signatures and should have minimum signatures update window of every one hour
	All the protection signatures should be created by vendor based on their threat intelligence and should not use any 3rd party IPS or AV engines.
	Should perform stream-based Anti-Virus inspection and not store-and-forward traffic inspection to keep the maximum firewall performance. Stream based Antivirus scanning should be used for scanning the contents of the files being transferred over the wire for virus/malwares and should block the file transfer when a virus or malware signatures is triggered.
	Should be able to perform Anti-virus scans for SMB traffic
	Should support DNS sink holing for malicious DNS request from inside hosts to outside bad domains and should be able to integrate and query third party external threat intelligence databases to block or sinkhole bad IP address, Domain and URLs
	Should be able to call 3rd party threat intelligence data on malicious IPs, URLs and Domains to the same firewall policy to block those malicious attributes and list should get updated dynamically with latest data
	Vendor should automatically push dynamic block list with latest threat intelligence database on malicious IPs, URLs and Domains to the firewall policy as an additional protection service
	Solution must prevent sensitive information such as credit card or social security numbers from leaving a protected network from day one. It should also allow administrator to filter on key words, such as a sensitive project name or the word confidential.
	Solution must prevent sensitive information such as credit card or social security numbers from leaving a protected network from day one. It should also allow administrator to filter on key words, such as a sensitive project name or the word confidential.
	The NGFW should prevent credential theft attack. Vendor should provide features with the ability to prevent the theft and abuse of stolen credentials, one of the most common methods of cyber adversaries use to successfully compromise and maneuver within an organization to steal valuable assets. It should also complement additional malware and threat prevention and secure application enablement functionality, to extend customer organizations' ability to prevent cyber breaches. · Automatically identify and block phishing sites · Prevent users from submitting credentials to phishing sites · Prevent the use of stolen credential
Advanced Persistent Threat (APT) Protection	This should have Inline prevention capabilities to stop patient zero threats without affecting productivity.
	The proposed solution should have signatureless approach to prevent unknown weaponized files, credential phishing, and malicious scripts instantly / real time without holding files or web pages without configuring MTA or sending to cloud for analysis.
	The proposed solution should identify variants of known malware in real-time without sending to cloud for analysis.
	This should be a cloud base unknown malware analysis service with guaranteed protection signature delivery time not more than ten seconds
	Advance unknown malware analysis engine should be capable of machine learning with static

Signature & Seal of the bidder

Description	Technical Specifications 2 Unit Utility Next-Generation Firewall
	analysis and dynamic analysis engine with custom-built virtual hypervisor analysis environment
	Advance unknown malware analysis engine with real hardware, detecting VM-aware malware to detect and protect from on-premise /virtual sandbox evading advance unknown malware
	Cloud base unknown malware analysis service should be certified with SOC2 or any other Data privacy compliance certification for customer data privacy protection which is uploaded to unknown threat emulation and analysis
	Cloud base unknown malware analysis service should be able to perform dynamic threat analysis on such as EXEs, DLLs, ZIP files, PDF documents, Office Documents, Java®, Android APKs, Adobe Flash applets, Web pages that include high-risk embedded content like JavaScript, Adobe Flash files. MAC OS and DMG file types
	The proposed next generation security platform should be able to detect and prevent zero-day threats infection through HTTP, HTTPS, FTP, SMTP, POP3, IMAP use by any of application used by the users (eg: Gmail, Facebook, MS outlook)
	Advance unknown malware analysis engine with real hardware, detecting VM-aware malware to detect and protect from virtual sandbox evading advance unknown malware
	Solution should detonate evasive threats in a real hardware environment, entirely removing an adversary's ability to deploy anti-VM analysis techniques
	Advance unknown malware analysis engine should be able to creates automated high-fidelity signature for command and control connections and spyware to inspect command and control http payload to create one to many payload base signatures protection from multiple unknown spyware and command and control channels using single content base signature
	The protection signatures created base unknown malware emulation should be payload or content base signatures that could block multiple unknown malware that use different hash but the same malicious payload.
SSL/SSH Decryption	The proposed firewall shall be able to identify, decrypt and evaluate SSL traffic in an outbound connection (forward-proxy)
	The proposed firewall shall be able to identify, decrypt and evaluate SSL traffic in an inbound connection
	The proposed firewall shall be able to identify, decrypt and evaluate SSH Tunnel traffic in an inbound and outbound connections
	The NGFW shall support the ability to have a SSL inspection policy differentiate between personal SSL connections i.e. banking, shopping, health and non-personal traffic
	SSL decryption must be supported on any port used for SSL i.e. SSL decryption must be supported on non-standard SSL port as well
	The NGFW shall support TLS version 1.3
Network Address Translation	The proposed firewall must be able to operate in routing/NAT mode
	The proposed firewall must be able to support Network Address Translation (NAT)
	The proposed firewall must be able to support Port Address Translation (PAT)
	The proposed firewall shall support Dual Stack IPv4 / IPv6 (NAT64, NPTv6)
	Should support Dynamic IP reservation, tunable dynamic IP and port over subscription
IPv6 Support	L2, L3, Tap and Transparent mode
	Should support on firewall policy with User and Applications
	Should support SSL decryption on IPv6
	Should support SLAAC Stateless Address Auto configuration
Routing and Multicast support	The proposed firewall must support the following routing protocols: - Static - RIP V1/V2 - OSPFv2/v3 with graceful restart - BGP v4 with graceful restart
	Policy-based forwarding
	PIM-SM, PIM-SSM, IGMP v1, v2, and v3
	Bidirectional Forwarding Detection (BFD)
Authentication	should support the following authentication protocols: - LDAP - Radius (vendor specific attributes) - Token-based solutions (i.e. Secure-ID) - Kerberos
	The proposed firewall's SSL VPN shall support the following authentication protocols - LDAP - Radius - Token-based solutions (i.e. Secure-ID) - Kerberos - SAML

Signature & Seal of the bidder

Description	Technical Specifications 2 Unit Utility Next-Generation Firewall
	- Any combination of the above
Monitoring, Management and Reporting	Should support on device management with complete feature parity on firewall administration
	Should have real time logging based on all Traffic, Threats, User IDs, URL filtering, Data filtering, Content filtering, unknown malware analysis, Authentication, Tunneled Traffic and correlated log view base on other logging activities
	Should support the report generation on a manual or schedule (Daily, Weekly, Monthly, etc.) basis
	Should allow the report to be exported into other format such as PDF, HTML, CSV, XML etc.
	Should have built in report templates based on Applications, Users, Threats, Traffic and URLs
	Should be able to create report based on SaaS application usage
	Should be able to create reports based on user activity
	Should be able to create custom report based on custom query base any logging attributes
	On-device management service should be able to provide all the mentioned features in case of central management server failure
Authorization	Original Manufacturer Authorization Certificate to be submitted along with the bid
	3 Years OEM Premium support bundle including parts & labor with 24x7x365 days TAC support, RMA, software updates and subscription update support. The NGFW should be proposed with 3 years subscription licenses for (i) Zero-Day Threat Protection (ii) NGFW (iii) NGIPS (iv) Anti-Virus (v) Anti Spyware, (vi) Anti Botnet and (vii) Anti APT
Cross Reference	Bidders has to provide public reference documents/links for each specification points mentioned in the above for verification.

** The above-mentioned price is inclusive of all costs, taxes & VATs as per rule of the government of Bangladesh.

Name of the Bidder :
Designation of the Bidder :
Company Name :
Business Address :
Mobile No. :

Signature & Seal of the bidder